WHAT IS CLAIMED IS:

1. A system to maintain application data stored on a portable computer secure, the system comprising:

an authorization client for use on the portable computer for making requests, the portable computer being capable of providing in-memory portions of address space for an application program;

a security device to be associated with an authorized user of the portable computer and including an authorization server for supplying responses to the requests;

a communication subsystem for wirelessly communicating the requests and the responses to the server and the client, respectively, within a range; and

a cryptographic subsystem for encrypting data located in the in-memory portions of the address space to obtain corresponding encrypted data when the security device is outside the range of the communication subsystem and for decrypting the encrypted data when the security device is back within the range.

2. The system as claimed in claim 1 wherein the requests include cryptographic requests for cryptographic information and wherein the server supplies the cryptographic information in response to the cryptographic requests and wherein the cryptographic subsystem utilizes the cryptographic information to either encrypt or decrypt the data.

3. The system as claimed in claim 1 further comprising means for suspending substantially all authorized user processes on the computer when the security device is outside the range and means for restarting the suspended authorized user processes on the computer when the security device is back within the range.

4. The system as claimed in claim 2 wherein the cryptographic information includes keys.

5. The system as claimed in claim 4 wherein the keys are encrypted.

6. The system as claimed in claim 1 further comprising means for suspending selected authorized user processes on the computer when the security device is outside the range and means for restarting the selected authorized user processes on the computer when the security device is back within the range.

7. The system as claimed in claim 1 further comprising a mechanism for establishing a binding between the portable computer and the security device to ensure that the security device only responds to a portable computer with a valid binding.

8. The system as claimed in claim 1 wherein the security device is an authorization token.

9. The system as claimed in claim 4 wherein the keys include at least one master key.

10. The system as claimed in claim 9 wherein the at least one master key is a key-encrypting key.

11. The system as claimed in claim 2 wherein the cryptographic subsystem includes encrypted keys and wherein the cryptographic information includes keys for decrypting the encrypted keys.

12. A method to maintain application data stored on a portable computer secure, the method comprising:

providing an authorization client for use on the portable computer for making requests, the portable computer being capable of providing in-memory portions of address space for an application program;

providing a security device to be associated with an authorized user of the portable computer and including an authorization server for supplying responses to the requests;

wirelessly communicating the requests and the responses to the server and the client, respectively, within a range;

encrypting data located in the in-memory portions of the address space to obtain corresponding encrypted data when the security device is outside the range; and

decrypting the encrypted data when the security device is back within the range.

13. The method as claimed in claim 12 further comprising suspending substantially all authorized user processes on the computer when the security device is outside the range and restarting the suspended authorized user processes on the computer when the security device is back within the range.

14. The method as claimed in claim 12 wherein the requests include cryptographic requests for cryptographic information and wherein the server supplies the cryptographic information in response to the cryptographic requests and wherein the cryptographic information is used to either encrypt or decrypt the data.

15. The method as claimed in claim 12 further comprising establishing a binding between the portable computer and the security device to ensure that the security device only responds to a portable computer with a valid binding.

16. The method as claimed in claim 12 further comprising suspending selected authorized user processes on the computer when the security device is outside the range and restarting the selected authorized user processes on the computer when the security device is back within the range.

17. The method as claimed in claim 14 wherein the cryptographic information includes keys.

18. The method as claimed in claim 17 wherein the keys include at least one master key.

19. The method as claimed in claim 18 wherein the at least one master key is a key-encrypting key.

20. An authorization token for use in a system to maintain application data stored in in-memory portions of address space on a portable computer secure, the token comprising:

an authorization server for supplying encrypted responses to encrypted requests; and

a transceiver for receiving the requests and transmitting the responses to the portable computer.

21. The token as claimed in claim 20 wherein the requests include cryptographic requests for cryptographic information and wherein the server supplies the cryptographic information in response to the cryptographic requests.

22. The token as claimed in claim 21 wherein the cryptographic information includes keys.

23. The token as claimed in claim 22 wherein the keys are encrypted.

24. The token as claimed in claim 22 wherein the keys include at least one master key.

25. The token as claimed in claim 24 wherein the at least one master key is a key-encrypting key.